UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,817	07/16/2003	Stephen F. Bisbee	003670-104	1237

7590 01/03/2007

Burns, Doane, Swecker & Mathis, L.L.P.
P.O. Box 1404
Alexandria, VA 22313-1404

EXAMINER	
LOVING, JARIC E	
ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/03/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/620,817	BISBEE ET AL.	
	Examiner	Art Unit	
	Jaric Loving	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This office action is responsive to Applicant's amendment received on October 3, 2006.

2. Applicant's arguments filed on October 3, 2006 have been fully considered, but they are not persuasive.

Information Disclosure Statement

3. The information disclosure statement contains non-patent literature ("NPL") documents that were not considered because they were not provided with the application. Furthermore, applicant refers to application 09/839,551 as a basis to refrain from providing the relevant NPL documents. However, applicant did not claim priority to that document and therefore, the NPL documents cited should have been provided.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-15, 19, 22-24, and 26-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Koehler, US 6,301,658.

In claim 1, Koehler discloses a method of providing a Certificate Status Service ("CSS") for checking validities of authentication certificates issued by respective issuing Certification Authorities ("CAs"), comprising the steps of:

identifying information needed for retrieving a status of an authentication certificate from an issuing CA that issued the authentication certificate (col. 5, lines 14-20);

configuring a connector based on the identified information for communicating with the issuing CA (col. 5, lines 46-50);

communicating with the issuing CA according to the configured connector when the status of the authentication certificate is queried (col. 5, lines 53-55); and

retrieving the status of the authentication certificate (col. 5, lines 53-55; col. 6, lines 1-3);

wherein the issuing CA and the connector are designated on a list of approved CAs in a configuration store (col. 6, lines 3-8).

In claim 2, Koehler discloses the method of claim 1, wherein a local date and time are checked for whether they fall within a validity period indicated in the authentication certificate and an invalid status is reported if the local date and time fall outside the validity period (col. 5, line 65 – col. 6,line 3).

In claim 3, Koehler discloses the method of claim 1, wherein the issuing CA is included in the list of approved CAs by vetting and approving the issuing CA according to predetermined business rules, and if the issuing CA is vetted and not approved, the

issuing CA is designated on a list of not-approved CAs in the configuration store (col. 5, lines 21-36; col. 8, lines 16-21).

In claim 4, Koehler discloses the method of claim 3, wherein vetting and approving the issuing CA includes registering a representation of a trusted authentication certificate with the CSS and adding at least the representation, status and a time-to-live data element to a local cache memory, and a connector is configured for retrieving the added status when the status of the trusted authentication certificate is queried (col. 7, lines 12-16 – timestamp provides a time to live; col. 8, lines 21-36).

In claim 5, Koehler discloses the method of claim 2, further comprising the steps of checking a local cache memory for the status, and if the status is found in the local cache memory and the local date and time are within the validity period, retrieving the status from the local cache memory, wherein if the status is not found in the local cache memory, the CSS establishes a communication session with a certificate status reporting component of the issuing CA, composes a certificate status request according to the configured connector, retrieves the status from the certificate status reporting component, closes the communication session with certificate status reporting component, and adds at least the authentication certificate's identification, status, and time-to-live to the local cache memory (col. 5, line 65 – col. 6, line 27).

In claim 6, Koehler discloses the method of claim 1, wherein the certificate status is indicated by a Certificate Revocation List (CRL), according to a publication schedule of the issuing CA, the CSS retrieves the CRL from a certificate status reporting component listed in the configuration store, the CSS clears a cache memory associated

with the issuing CA, and the CSS determines the status of the authentication certificate from the CRL and stores the status in the cache memory associated with the issuing CA (col. 5, line 65 – col. 6, line 27 – verification server can also consider CRL of CA).

In claim 7, Koehler discloses the method of claim 1, wherein the certificate status is indicated by a Delta Certificate Revocation List ("ΔCRL"); upon notification by the issuing CA that a ΔCRL is available, the CSS retrieves the ΔCRL from a certificate status reporting component listed in the configuration store; if the ΔCRL is a complete CRL, then the CSS clears a cache memory associated with the issuing CA, determines the status from the CRL, and stores the status in the cache memory; and if the ΔCRL contains only changes occurring after publication of a full CRL, the CSS determines the status from the ΔCRL, and stores the status in the cache memory (col. 7, lines 12-34).

In claim 8, Koehler discloses the method of claim 1, wherein the communicating step includes communicating according to a sequence of connectors (col. 5, lines 42-46; col. 8, lines 37-45).

In claim 9, Koehler discloses the method of claim 1, wherein a connector embeds more than one certificate status check in a single communicating step (col. 5, lines 42-46; col. 8, lines 37-45).

In claim 10, Koehler discloses the method of claim 1, wherein the authentication certificate is not used for identification (col. 5, lines 42-46; col. 8, lines 37-45).

In claim 11, Koehler discloses a method of retrieving a status of an authentication certificate issued by an issuing Certification Authority ("CA") in response to a query from

a trusted third-party repository of information objects to a Certificate Status Service ("CSS") to validate the authentication certificate's status, comprising the steps of:

locating and reporting the status if the status is present and current in a cache memory of the CSS (col. ,line 63 – col. 6, line 8);

otherwise performing the steps of:

obtaining a status type and retrieval method from a CSS configuration store (col. ,line 63 – col. 6, line 8);

if the status type is Certificate Revocation List ("CRL") and the last retrieved CRL is current, but the status is not found in the cache memory, then reporting the status as valid (col. 6, lines 9-27);

if the status type is not CRL, then composing a certificate status request according to the status type (col. 6, lines 9-27 – if no entry, status composed from repository);

establishing a communication session with the issuing CA (col. 5, lines 48-55; col. 6, lines 28-41);

retrieving the status from a status reporting component of the issuing CA using the obtained retrieval method and ending the communication session (col. 6, lines 56-66);

interpreting the retrieved status (col. 6, lines 56-66);

associating, with the interpreted retrieved status, a time-to-live value representing a period specified by a CSS policy for the status type (col. 6, lines 56-66);

adding at least the authentication certificate's identification, status, and time-to-live values to the cache memory (col. 5, line 63 – col. 6, line 8); and

reporting the status to the trusted third-party repository of information objects in response to the query (col. 8, lines 2-21).

In claim 12, Koehler discloses the method of claim 11, wherein the CSS uses a certificate status protocol in the communication session (col. 5, lines 44-48).

In claim 13, Koehler discloses the method of claim 11, wherein more than one status is retrieved using the obtained retrieval method (col. 5, lines 42-48).

In claim 14, Koehler discloses the method of claim 11, wherein the authentication certificate is not used for identification (col. 5, lines 42-46; col. 8, lines 37-45).

In claim 15, Koehler discloses a Certificate Status Service ("CSS") for providing accurate and timely status indications of authentication certificates issued by issuing Certification Authorities ("CAs"), comprising:

providing a status of an authentication certificate as indicated by a Certificate Revocation List ("CRL") when the certificate's issuing CA uses CRLs for indicating status (col. 7, lines 12-34);

otherwise, providing the status indicated by a cache memory when the cache memory includes a status and a time-to-live data element is not exceeded (col. 7, lines 17-19);

if the time-to-live data element is exceeded, clearing the status from the cache memory (col. 5, lines 47-49);

requesting and retrieving the status using a real-time certificate status reporting protocol when the status is not in the cache memory (col. 5, lines 53-55);

adding at least the certificate's identification, status, and time-to-live data element to the cache memory (col. 5, line 63 – col. 6, line 8); and

providing the retrieved status (col. 5, line 63 – col. 6, line 8).

In claim 19, Koehler discloses a method of executing a transaction between a first party and a second party by transferring control of an authenticated information object having a verifiable evidence trail, comprising the steps of:

retrieving an authenticated information object from a trusted repository, wherein the authenticated information object includes a first digital signature block comprising a digital signature of a submitting party and a first authentication certificate relating at least an identity and a cryptographic key to the submitting party, a date and time indicator, and a second digital signature block comprising a second digital signature of the trusted repository and a second authentication certificate relating at least an identity and a cryptographic key to the trusted repository; the first digital signature block was validated by the trusted repository; and the authenticated information object is stored as an electronic original information object under the control of the trusted repository (col. 7, line 66 – col. 8, line 21 – root has authentication authority of other CAs);

executing the retrieved authenticated information object by the second party by including in the retrieved authenticated information object a third digital signature block comprising at least a third digital signature and a third authentication certificate of the second party (col. 7, line 66 – col. 8, line 21); and

forwarding the executed retrieved authenticated information object to a trusted third-party repository of information objects, wherein the trusted third-party repository of information objects verifies digital signatures and validates authentication certificates associated with the digital signatures included in information objects by at least retrieving status of the authentication certificates from a Certificate Status Service ("CSS") provided according to claim 1; the trusted third-party repository of information objects rejects a digital signature block if the respective digital signature is not verified or the status of the respective authentication certificate is expired or is revoked; and if at least one signature block in the information object is not rejected, the trusted third-party repository of information objects appends the trusted third-party repository's digital signature block and a date and time indicator to the information object and takes control of the object on behalf of the first party (col.5 ,lines 53-55; col. 5, line 63 – col. 6, line 8; col. 7, line 66 – col. 8, line 21).

In claim 22, Koehler discloses the method of claim 19, wherein if the trusted third-party repository of information objects rejects a digital signature block, the trusted third-party repository of information objects requests a remedy that requires the digital signature to be recomputed and the signature block to be reforwarded (col. 6, lines 33-51).

In claim 23, Koehler discloses the method of claim 19, wherein the trusted third-party repository of information objects checks the local date and time for accuracy and that they are within a validity period indicated by the second party's authentication certificate (col. 6, lines 33-51 – root CA checks timestamp).

In claim 24, Koehler discloses the method of claim 23, wherein if the local date and time are not within the validity period indicated by the second party's authentication certificate, the trusted third-party repository of information objects notifies the second party that the authentication certificate is rejected and the first party that the transaction is incomplete (col. 6, lines 30-33).

In claim 26, Koehler discloses the method of claim 19, wherein one or more digitized handwritten signatures are included in the information object, and placement of the digitized handwritten signatures in a data structure is specified by at least one signature tag (col. 4, line 66 – col. 5, line 20).

In claim 27, Koehler discloses the method of claim 26, wherein one or more signature blocks are separately forwarded to the trusted third-party repository of information objects with respective signature tags, and the trusted third-party repository of information objects validates the signature blocks by:

rejecting a signature block if either the respective digital signature is not verified or the respective authentication certificate is not validated (col. 5, lines 27-29; col. 5, line 63 – col. 6, line 8), and

placing the signature block according to the respective signature tag if the signature block is not rejected (col. 5, lines 2-20 – timestamp is entered according to whether it is expired, also public keys are entered based on validity),

wherein, to signature blocks sent separately, the trusted third-party repository of information objects adds a date and time indication to each signature block and appends according to business rules the trusted third-party repository's signature block

in a wrapper that encompasses the information object and placed signature blocks (col. 5, line 63 – col. 6, line 3).

In claim 28, Koehler discloses the method of claim 27, wherein the trusted third-party repository of information objects verifies a digital signature and validates an authentication certificate in a signature block by:

determining from the business rules whether a party associated with the authentication certificate has authority (col. 5, lines 14-15),

verifying the party's digital signature, checking that the authentication certificate's validity period overlaps the trusted third-party repository's current date and time (col. 5, lines 17-20),

checking that the local date and time falls within an allowable deviation from the trusted third-party repository's current date and time (col. 5, lines 8-10), and

retrieving status of the authentication certificate from the CSS (col. 5, line 63 – col. 6, line 3), and

if any of the preceding steps results in an invalid or false output, the digital signature is deemed invalid, the transaction is not executed, otherwise the digital signature is deemed valid and the transaction is executed (col. 6, lines 28-51).

In claim 29, Koehler discloses the method of claim 19, wherein the CSS provides authentication certificate status to the trusted third-party repository of information objects by at least the steps of checking a local cache memory for the status, and if the status is found in the local cache memory and the local date and time are within the validity period, and retrieving the status from the local cache memory; if the status is not

found in the local cache memory or if the local date and time are not within the validity period, the CSS establishes a communication session with a certificate status reporting component of the issuing CA, composes a certificate status request trusted third-party repository of information objects, retrieves the status from the certificate status reporting component, closes the communication session with certificate status reporting component, and adds at least the authentication certificate's identification, status, and a time-to-live data element to the local cache memory (col. 5, lines 48-55; col. 5, line 65 – col. 6, line 8).

In claim 30, Koehler discloses the method of claim 19, wherein the first party is a first trusted third-party repository of information objects and the transaction is for transferring custody of one or more electronic originals to the first trusted third-party repository of information objects from a second trusted third-party repository of information objects, an owner of the transaction provides the second trusted third-party repository of information objects with a manifest that identifies electronic originals to be transferred to the first trusted third-party repository of information objects, the second trusted third-party repository of information objects establishes communication with the first trusted third-party repository of information objects and identifies the purpose of its actions, the manifest is communicated to the first trusted third-party repository of information objects so that it is able to determine when the transfer of custody has been completed, the second trusted third-party repository of information objects transfers each identified electronic original to the first trusted third-party repository of information objects, the first trusted third-party repository of information objects retrieves status of

the second trusted third-party repository's certificate and verifies the second trusted third-party repository's digital signature on each transferred electronic original, if any of the second trusted third-party repository's digital signatures or certificates are invalid, then the first trusted third-party repository of information objects notifies the second trusted third-party repository of information objects and seeks a remedy, if the second trusted third-party repository of information objects does not provide a remedy, the first trusted third-party repository of information objects notifies the transaction owner that the requested transfer of custody has failed, otherwise the second trusted third-party repository of information objects creates a new wrapper for each successfully transferred information object, adding a date-time stamp and the first trusted third-party repository's signature block (col. 6, lines 28-55; col. 8, lines 2-36).

In claim 31, Koehler discloses the method of claim 30, wherein the transaction is a transfer of ownership in response to an instruction, transfer of ownership documentation is placed in either the first trusted third-party repository of information objects or the second trusted third-party repository of information objects, the trusted third-party repository of information objects having the transfer of ownership documentation validates authenticity of the transfer of ownership documentation by verifying all digital signatures, certificate validity periods, and using the CSS to check certificate status of all authentication certificates included in the transfer of ownership documentation, appends a date and time indication, and digitally signs, wraps and stores the transfer of ownership documentation, which are added to the manifest (col. 6, lines 28-55; col. 8, lines 2-36).

In claim 32, Koehler discloses the method of claim 19, wherein the certificate status is indicated by a Certificate Revocation List (CRL), according to a publication schedule of the issuing CA, the CSS retrieves the CRL from a certificate status reporting component listed in the configuration store, the CSS clears a cache memory associated with the issuing CA, and the CSS determines the status of the authentication certificate from the CRL and stores the status in the cache memory associated with the issuing CA (col. 5, line 65 – col. 6, line 27).

In claim 33, Koehler discloses the method of claim 19, wherein the certificate status is indicated by a Delta Certificate Revocation List ("ΔCRL"); upon notification by the issuing CA that a ΔCRL is available, the CSS retrieves the ΔCRL from a certificate status reporting component listed in the configuration store; if the ΔCRL is a complete CRL, then the CSS clears a cache memory associated with the issuing CA, determines the status from the CRL, and stores the status in the cache memory; and if the ΔCRL contains only changes occurring after publication of a full CRL, the CSS determines the status from the ΔCRL, and stores the status in the cache memory (col. 7, lines 12-34).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koehler and further in view of Konheim, US 4,264,782.

In claim 16, Koehler fails to disclose a status use-counter data element is added to the cache memory; the status use-counter data element is incremented or decremented every time the certificate's status is checked; and if the status use-counter data element passes a threshold, then the status is provided and the cache memory is cleared with respect to the status. Konheim discloses a status use-counter data element is added to the cache memory; the status use-counter data element is incremented or decremented every time the certificate's status is checked; and if the status use-counter data element passes a threshold, then the status is provided and the cache memory is cleared with respect to the status (col. 11, lines 58-68; col. 12, lines 37-47).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Koehler's digital certificate authentication system with Konheim's identity verification method utilizing a use-counter to check memory access. It is for this reason that one of ordinary skill in the art would have been motivated to provide Koehler's digital certificate authentication system with a use-counter because it protects against the re-use of a previously verified transaction (Konheim, col. 7, lines 4-6).

In claim 17, Koehler, as modified, discloses the CSS of claim 16, wherein a status last-accessed data element is added to the cache memory, and the status last-accessed data element in conjunction with the status use-counter data element enable determination of an activity level of the certificate's status (Koehler, col. 6, lines 17-22).

In claim 18, Koehler, as modified, discloses the CSS of claim 17, wherein when a request is made to the CSS to retrieve a status of a new certificate and the cache

memory has reached an allocated buffer size limit, the CSS searches the cache memory for a least-accessed data element indicating an oldest date and clears the respective cache memory entry; and the CSS then retrieves the requested status, places it in the cache memory, and provides the requested status (col. 6, lines 12-27; col. 7, lines 52-57 – updates timestamp which thus clears the memory and enters a new value).

5. Claims 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koehler and further in view of Kocher, US 5,903,651.

In claim 20, Koehler fails to disclose a signature block including at least one hash of at least a portion of the information object in which the signature block is included, the at least one hash is encrypted by the cryptographic key of the block's respective signer, thereby forming the signer's digital signature, and the signer's digital signature is included in the signature block with the signer's authentication certificate. Kocher discloses a signature block including at least one hash of at least a portion of the information object in which the signature block is included, the at least one hash is encrypted by the cryptographic key of the block's respective signer, thereby forming the signer's digital signature, and the signer's digital signature is included in the signature block with the signer's authentication certificate (col. 4, lines 23-26 and lines 41-45).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Koehler's digital certificate authentication system with Kocher's method of confirming certificate status utilizing hashing a portion of information to create more secure data transfers. It is for this reason that one of ordinary skill in the art would

have been motivated to provide Koehler's digital certificate authentication system with hashing because it allows certificate status to be determined without knowledge of an entire list of revoked certificates (Kocher, col. 3, lines 29-32 and lines 59-61).

In claim 21, Koheler, as modified, discloses the method of claim 20, wherein the executing step includes displaying a local date and time to the second party, affirming, by the second party, that the displayed local date and time are correct, and correcting the local date and time if either is incorrect (Koehler, col. 7, lines 43-57).

6. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Koehler and further in view of Smithies et al., US 5,818,955.

In claim 25, Koehler fails to disclose one or more digitized handwritten signatures are included in the information object, and placement of the digitized handwritten signatures in a data structure is specified by at least one signature tag. Smithies discloses one or more digitized handwritten signatures are included in the information object, and placement of the digitized handwritten signatures in a data structure is specified by at least one signature tag (col. 3, lines 39-49).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Koehler's digital certificate authentication system with Smithies signature verification method utilizing digitized handwritten signatures to allow a user to store a handwritten signature. It is for this reason that one of ordinary skill in the art would have been motivated to provide Koehler's digital authentication system with digitized handwritten signatures because it allows a person to determine whether two signatures are from the same person (Smithies, col. 3, lines 12-18).

Response to Arguments

4. Regarding claims 1-33, Applicant basically argues the Koehler reference is inapplicable and the Konheim, Kocher, and Smithie patents do not cure the deficiencies of the Koehler reference.

As to claim 1, Applicant argues "the Koehler patent would not have taught or suggested identifying information needed for retrieving a status of an authentication certificate from an issuing CA that issued the authentication certificate." Examiner contends Koehler does disclose this limitation. In col. 5, lines 16-20, Koehler provides "CA digital signature 40 is the digital signature of the issuing certificate authority and is used to verify that certificate 10 is authentic and indeed issued by the authority identified in CA information." The digital signature provides identifying information from the CA that issued the certificate.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., multiple individual CAs or CA hierarchies) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Next, Applicant argues Koehler does not disclose "configuring a connector based on the identified information for communicating with the issuing CA." Examiner contends Koehler does disclose this limitation. In col. 5, lines 46-50, Koehler provides "[v]erification server 60 receives verification requests 90 from a plurality of clients."

Therefore, the server acts as a connector to allow the clients to communicate with the CA based on verification information.

Next, Applicant argues Koehler does not disclose "communicating with the issuing CA according to the configured connector when the status of the authentication certificate is queried." Examiner contends Koehler does disclose this limitation. In col. 5, lines 53-55, Koehler provides "[v]erfiication server 60 receives each client request 90 and responds whether a particular digital certificate is authentic." Thus, the server communicates when authentication of the certificate is performed.

Next, Applicant argues Koehler does not disclose "retrieving the status of the authentication certificate. Examiner contends Koehler does disclose this limitation. In col. 5, lines 53-55 and col. 6, lines 1-3, the server determines the validity and thus the status of the authentication certificate.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., risk management means and business rules can force status updates or clearing of status based on the number of times a certificate's status is queried, or other criteria, which may differ based on community or application) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Next, Applicant argues Koehler does not disclose "the issuing CA and the connector are designated on a list of approved CAs in a configuration store." Examiner

contends Koehler does disclose this limitation. In col. 6, lines 3-8, Koehler describes a verification cache where an entry contains information such as issuer and user privileges. Thus, a list of approved CAs are stored in the cache.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., excluding an individual CA or CA hierarchy) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

As to claim 2, Applicant argues "Koehler would not have taught or suggested checking to see if local time is beyond the certificate's validity period." Examiner contends Koehler does disclose this limitation. In col. 5, line 65 – col. 6, line 3, Koehler describes the verification server as utilizing timestamp to determine the validity of certificates in the cache. This suggests the server would determine whether the time checked is either within or outside a valid time period.

As to claim 3, Applicant argues "[t]he Koehler disclosure does not relate to maintaining a list of approved and disapproved CAs" and "would not have taught or suggested excluding specific CAs." Examiner contends otherwise. In col. 5, lines 21-36 and col. 8, lines 16-21, Koehler describes the use of a certificate revocation list within a CA hierarchy. Therefore, a non-approved CA would be placed on the revocation list while approved CAs are those not on the revocation list, but still within a given hierarchy.

As to claim 4, Applicant argues "[t]he Koehler disclosure does not relate to vetting, approving, documenting, and implementing means of communicating with approved CAs to retrieve queried certificate's status." Examiner contends otherwise. In col. 8, lines 21-36, Koehler describes checking the validity of the issuing CA certificate and checks the CRL. If the CA is not in the CRL, the status of the certificate would be known.

As to claim 5, Applicant argues "[t]he Koehler disclosure of a verification timestamp would not have taught or suggested the claimed time-to-live indicator with the CSS enforced policies and practices and/or communications load mitigation." Examiner contends otherwise. In col. 5, line 65 – col. 6, line 27, Koehler describes using the timestamp to determined whether a certificate is still valid and maintains this information in a cache. Therefore, the timestamp provides a time-to-live indicator based on the certificate issuers policies. The server also updates the cache with a new entry, if an unauthenticated item requests verification.

As to claim 6, Applicant argues Koehler does not disclose the method of claim 6. Examiner contends otherwise. In col. 5, line 65 – col. 6, line 27, Koehler describes whether a certificate is still valid by checking timestamp information and a CRL. The verification server will authenticate a certificate by checking the cache and if not present will obtain information from a repository for entry in the cache and update it with a timestamp.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies

(i.e., any other certificate status reporting protocols; retrieving status in which a number of algorithms can be employed to optimize cache and reduce system overhead) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

As to claim 7, Applicant argues Koehler is silent on ΔCRL retrieval. Examiner contends otherwise. On page 21, lines 14-16, Applicant's specification provides that a "Delta CRL may be generated whenever a certificate is revoked or suspended during the interval between publications of the full CRLs. Delta CRLs may contain a complete list of revoked CRLs." In col. 12, lines 12-34, Koehler describes where a CA CRL is utilized when a certificate is not valid under a CRL. The CA CRL information is updated in the cache after the verification server authenticates the certificate. The CA CRL is not the same as the CRL and thus may have changes apart from a full CRL or contains all the information in the CRL. Therefore, the CA CRL behaves similarly to the Delta CRL.

As to claim 8, Applicant argues "Koehler would not have taught or suggested the [features of claim 8]." Examiner contends Koehler does disclose the limitation. In col. 5, lines 42-46 and col. 8, lines 37-45, Koehler describes the verification server as communicates with the cache and CAs within the hierarchy.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., connectors to communicate with multiple independent CAs) are not recited in the

rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

As to claim 9, applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., employing communications overhead reduction techniques such as nesting certificate status requests for a multi-party transaction where at least two parties have certificates issued by the same CA) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

As to claim 10, applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., CSS which supports certificates used for purposes other than proof of identity such as attributes certificates or certificates used for encrypting storage media) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

As to claim 11, Applicant argues "Koehler... is silent on trusted third-party repository of information objects" and "Koehler... is silent as to how the status is obtained from CAs that are not a member of the CA hierarchy or that are a certificate status reporting service other than a CA." Examiner contends otherwise. In col. 5, lines

44-62, Koehler provides that the verification server interacts with a certificate repository that may reside across a network and not necessarily connected directly to the server.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., how the status is obtained from CAs that are not a member of the CA hierarchy; a certificate status reporting service other than a CA) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Next, Applicant argues "[t]he Koehler patent doesn't disclose making use of a time-to-live value, and adds the validated certificate itself to cache" and "... Koehler would not have taught or suggested the CSS being used by a trusted third-party repository of information objects for obtaining certificate status." Examiner contends otherwise. In col. 5, lines 63 – col. 6, line 8, Koehler describes using a timestamp to determine whether a certificate is valid. Therefore, it utilizes a time-to-live value that is based on other CA certificate policies. In col. 5, lines 44-62 and col. 8, lines 2-21, Koehler describes the authentication hierarchy being connected to the verification server which interacts with the certificate repository that stores all information objects for certificate status.

As to claim 15, Applicant argues "...Koehler... is silent as to clearing of status based on a CSS' certificate status retention policy and business rules... silent as to the use of a real-time certificate status reporting protocol to retrieve certificate status for a

CA or certificate status reporting service" and "would not have taught or suggested the features of [claim 15]." Examiner contends otherwise. In col. 5, line 63 – col. 6, line 8, Koehler describes the timestamp being used to determine validity of a certificate. Elements of the certificate include expiration data which would indicate the status of the certificate is cleared. In col. 5, lines 53-55, Koehler states that the verification server responds whether a certificate is authentic when a client request is received. Therefore, the status of the issued CA is reported in real time.

As to claim 19, Applicant argues Koehler "is silent as to the execution of multi-party transactions...is silent on the use of the CSS... by a trusted third-party repository of information objects to obtain certificate status for digital signature block affixed to authenticated information objects that are received by the trusted third-party repository of information objects and the trusted third-party repository's handling of the authenticated information object based on the certificate status returned by the CSS" and "would not have taught or suggested" the features of claim 19. Examiner contends otherwise. In col. 5, lines 53-55; col. 5, line 53 – col. 6, line 8; col. 7, line 66 – col. 8, line 21, Koehler describes the verification server as responding whether a certificate is authentic. The server interacts with a certificate repository that maintains all certificates in the authentication hierarchy. Each certificate contains the signature of the issuing authority. Each CA in a hierarchy can validate the certificate of a subordinate CA. Further, timestamps and a CRL allow the repository to determine whether the certificate has been expired or revoked.

As to claim 22, Applicant argues Koehler "is silent on a trusted third-party repository of information objects requiring resubmission of any information object to be authenticated that does not have valid signature blocks" and "would not have taught or suggested the features recited in claim 22." Examiner contends otherwise. In col. 6, lines 33-51, Koehler provides "If [the item does not correspond to root CA], verification server... retrieves a digital certificate of the CA that issued the item being authenticated... if no [cache] entry exists, verification server 60 retrieves the CA certificate from certificate repository 80, creates a cache entry and sets its verified timestamp to an uninitialized state." Thus, if the certificate does not correspond to the root CA, the verification server will request the issuing CA to recompute the certificate and resend.

As to claim 23, Applicant argues Koehler "would not have taught or suggested [the] capabilities encompassed by claim 23." Examiner contends Koehler does disclose the limitations of claim 23. In col. 6, lines 33-51, the verification server checks to see whether the certificate has expired from the timestamp. Therefore, the date and time are checked.

As to claim 26, Applicant argues Koehler "is silent on the use and placement of digitized handwritten signatures." In col. 4, line 66 – col. 5, line 20, Koehler mentions the issuer's digital signature is included in the certificate. It is well known in the art that digital signature also encompasses digitized signatures.

As to claim 27, Applicant argues Koehler "is silent on a trusted third-party repository of information objects that is a secure repository of information objects and

that separately verifies digital signatures on submitted information objects prior to storing and controlling these information objects... silent on detaching signature blocks from content and forwarding only the signature block to the trusted third-party repository of information objects... silent on the handling and processing of detached signature blocks... silent on a trusted third-party repository of information objects using a wrapper or placement of signature blocks and information objects in wrappers." Examiner contends otherwise. In col. 5, lines 27-29, Koehler provides that part of the certificate verification process includes validating the digital signature to ensure authenticity. It is also stated that validation of the digital signature is a different validation process and therefore detached from other validation processes used to validate the certificate. In col. 5, line 63 – col. 6, line 8, Koehler discloses the certificate being stored in a cache, which are also contained in the certificate repository. Finally, each entry in the cache is given its own data file and thus a wrapper.

As to claim 28, Applicant argues Koehler "is silent on business rules or their use by the trusted third-party repository of information objects to check the authority of the identified party to perform actions... silent on the need for the trusted third-party repository of information objects to check the accuracy of local time." In col. 5, lines 8-20, Koehler describes the CA information within the certificate is used to verify the certificate's authenticity and thus provides rules on whether the issuing party has authority. In col. 5, lines 8-10 and col. 5, line 63 – col. 6, line 3, Koehler provides that the timestamp is used to determine the validity of the certificate. Thus, the certificate

repository can determine through the verification server as to the validity period of the certificate.

As to claim 29, Applicant argues Koehler does not disclose the elements of claim 29. Similar arguments have already been addressed to these components with respect to claims 1, 5, 6, 11, and 28.

As to claim 30, Applicant argues Koehler "is silent on validation of the initiating instruction and transfer-of-custody of authenticated information between trusted third-party repositories." Examiner contends otherwise. In col. 6, lines 28-55 and col. 8, lines 2-36, Koehler describes the verification server determining the validity of a certificate. Thus, it is validating the initial instruction, which is the certificate sent by the CA. Further, Koehler provides a CA hierarchy and transfers custody of a certificate by moving up a chain. The CA hierarchy and the verification server are all connected to certificate repository.

As to claim 31, Applicant argues Koehler "is silent on validation of the initiating instruction and transfer-of-ownership of authenticated information objects. Examiner contends otherwise. A similar argument has already been addressed with respect to claim 30.

The Konheim, Kocher, and Smithie patents were cited for the respective teachings not found in Koehler and were not applied in the claims discussed above.

The remaining dependent claims that depend from the independent claims discussed above follow the reasoning above.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jaric Loving whose telephone number is (571) 272-1686. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JL

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER